Grenada

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 12 September 2023

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Electronic Crimes Act 2013 as amended through Act no. 10 of 2014** **Interpretation** 2. In this Act- "data" includes representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system; "electronic" means relating to technology having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic, or similar capabilities; "electronic database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by an electronic system or electronic network and are intended for use in an electronic system or electronic network; "electronic device" is any hardware that accomplishes its functions using any form or combination of electrical energy; "electronic system" means an electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and includes an electronic storage medium; "traffic data" means any data relating to a communication by means of an electronic system, generated by an electronic system that formed a part in the chain of communication, indicating the communication's origin, destination, route,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	time, date, size, duration, or type of underlying service. **Electronic Evidence Act 2013** "computer" means any digital information system integrated by equipment and programs intended for creation, recording, storage, processing and/or transmission of data, including any computer, computer devices, or other electronic information or communication devices, intended to perform such functions; "data (or computer data, or electronic data)" means any representation of facts, information or concepts in a form suitable for processing in an information system including a program suitable for causing an informaiont system to perform a function; "electronic" includes created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic, optical or by any other means that has capabilities for creation, recording, transmission or storage similar to those means; "electronic communication" means any transfer of records by means of signs, signals, writing, images, sounds, data, or intelligence of any 102 Act 13 Electronic Evidence 2013 nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include– (a) any oral communication; (b) any communication made through a tone-only paging device; (c) any communication from a tracking device; "electronic record" means a set of data that is created, generated, recorded, stored, processed, sent, communicated, and/or received, on any physical medium by a computer or other similar device, that can be read or perceived by a person by means of a computer system or other similar device, including a display, print-out or other output of those data; "information system (or computer system, or data processing system)" means a device or a group of inter-connected or related devices, including the internet, one or more of which, pursuant to a program, performs automatic processing of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	data or any other function; "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user or a publicly available electronic communications service; "record" means recorded information collected, created or received in the initiation, conduct or completion of an activity and that comprises sufficient content, context and structure to provide evidence or proof of that activity or transaction, inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic or any other medium and is accessible in a perceivable form; "traffic data" means computer data that– (a) relates to a communication by means of a computer system; (b) is generated by a computer system that is part of the chain of communication; and (c) shows the communication's origin, destination, route, time, date, size, duration or type of underlying services.
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Electronic Crimes Act 2013** **Interpretation** "unauthorized access" means access of any kind by a person to an electronic system or data held in an electronic system which is unauthorized or done without authority or is in excess of authority, if the person is not himself entitled to control access of the kind in question to the electronic system or data and the person does not have consent to such access from a person so entitled. **Unauthorised access and interference** 5. (1) A person shall not knowingly or without lawful excuse or justification, or without permission of the owner or any other person who is in charge of an electronic system or network–

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) gain access or secure to such electronic system or network; (b) download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium; (c) introduce or cause to be introduced a contaminant or malicious code into an electronic system or network; (d) damage or cause to be damaged an electronic system or network, data, electronic database or other program residing in such electronic system or network; (e) disrupt or causes the disruption of an electronic system or network; (f) deny or cause the denial of access to a person authorised to obtain access to an electronic system or network by any means; (g) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act; (h) charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network; (i) willfully destroy, delete or alter data information residing in an electronic system or diminishes its value or utility of affects it injuriously by any means; or (j) steal, conceal, destroy or alter or cause a person to steal, conceal, destroy or alter any source code used for an electronic system with an intention of causing damage. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years, or to both. **Sensitive electronic system.** 13. (1) A person shall not knowingly or without lawful excuse or justification disable or obtain access to a sensitive electronic system whether or not in the course of the commission of another offence under this Act. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction on indictment to a fi ne not exceeding three hundred thousand dollars or to a term of imprisonment not exceeding twenty years or to both. (3) For the purposes of this section a "sensitive electronic system" is an electronic system used directly in connection with or necessary for– (a) the security, defence or international relations of Grenada; (b) the existence or identity of a confi dential source of information relating to the enforcement of criminal law; (c) the provision of services directly related to communications infrastructure, banking and fi nancial services, public utilities, courts, public transportation or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	public key infrastructure; (d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services; or (e) the purpose declared as such by the Minister by Order published in the Gazette. **Unauthorized access to code** 18. (1) A person shall not knowingly or without lawful excuse or justification disclose or obtain a password, an access code or any other means of gaining access to an electronic system or data for wrongful gain or to inflict loss to a person or for any unlawful purpose. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years or to both.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Electronic Crimes Act 2013** **Unauthorised access and interference** 5. (1) A person shall not knowingly or without lawful excuse or justification, or without permission of the owner or any other person who is in charge of an electronic system or network– (a) gain access or secure to such electronic system or network; (b) download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium; (c) introduce or cause to be introduced a contaminant or malicious code into an electronic system or network; (d) damage or cause to be damaged an electronic system or network, data, electronic database or other program residing in such electronic system or network; (e) disrupt or causes the disruption of an electronic system or network; (f) deny or cause the denial of access to a person authorised to obtain access to an electronic system or network by any means; (g) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act; (h) charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network; (i) willfully destroy, delete or alter data information residing in an electronic system or diminishes its value or utility of affects it injuriously by any means; or (j) steal, conceal, destroy or alter or cause a person to steal, conceal, destroy or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	alter any source code used for an electronic system with an intention of causing damage. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years, or to both. **Violation of privacy** 10. (1) A person who, knowingly or without lawful excuse or justification, captures, publishes or transmits the image of a private area of a person without his or her consent, under circumstances violating the privacy of that person, commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years or to both. (2) For the purposes of this section– (a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons; (b) "capture" with respect to an image, means to videotape, photograph, film or record by any means; (c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast; (d) "publishes" means reproduction in the printed or electronic form and making it available for public; (e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that – (i) he or she could disrobe in privacy, without being concerned that an image or his or her private area was being captured; or (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Electronic Crimes Act 2013** **Unauthorised access and interference** 5. (1) A person shall not knowingly or without lawful excuse or justification, or without permission of the owner or any other person who is in charge of an electronic system or network– (a) gain access or secure to such electronic system or network; (b) download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium; (c) introduce or cause to be introduced a contaminant or malicious code into an

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	electronic system or network; (d) damage or cause to be damaged an electronic system or network, data, electronic database or other program residing in such electronic system or network; (e) disrupt or causes the disruption of an electronic system or network; (f) deny or cause the denial of access to a person authorised to obtain access to an electronic system or network by any means; (g) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act; (h) charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network; (i) willfully destroy, delete or alter data information residing in an electronic system or diminishes its value or utility of affects it injuriously by any means; or (j) steal, conceal, destroy or alter or cause a person to steal, conceal, destroy or alter any source code used for an electronic system with an intention of causing damage. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years, or to both. **Sensitive electronic system.** 13. (1) A person shall not knowingly or without lawful excuse or justification disable or obtain access to a sensitive electronic system whether or not in the course of the commission of another offence under this Act. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction on indictment to a fi ne not exceeding three hundred thousand dollars or to a term of imprisonment not exceeding twenty years or to both. (3) For the purposes of this section a "sensitive electronic system" is an electronic system used directly in connection with or necessary for– (a) the security, defence or international relations of Grenada; (b) the existence or identity of a confi dential source of information relating to the enforcement of criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation or public key infrastructure; (d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services; or (e) the purpose declared as such by the Minister by Order published in the Gazette.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Electronic Crimes Act 2013** **Unauthorised access and interference** 5. (1) A person shall not knowingly or without lawful excuse or justification, or without permission of the owner or any other person who is in charge of an electronic system or network– (a) gain access or secure to such electronic system or network; (b) download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium; (c) introduce or cause to be introduced a contaminant or malicious code into an electronic system or network; (d) damage or cause to be damaged an electronic system or network, data, electronic database or other program residing in such electronic system or network; (e) disrupt or causes the disruption of an electronic system or network; (f) deny or cause the denial of access to a person authorised to obtain access to an electronic system or network by any means; (g) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act; (h) charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network; (i) willfully destroy, delete or alter data information residing in an electronic system or diminishes its value or utility of affects it injuriously by any means; or (j) steal, conceal, destroy or alter or cause a person to steal, conceal, destroy or alter any source code used for an electronic system with an intention of causing damage. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years, or to both.
Article 6 – Misuse of devices	**Electronic Crimes Act 2013**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	**Unauthorized access to code** 18. (1) A person shall not knowingly or without lawful excuse or justification disclose or obtain a password, an access code or any other means of gaining access to an electronic system or data for wrongful gain or to inflict loss to a person or for any unlawful purpose. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years or to both.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic,	**Electronic Crimes Act 2013** **Electronic forgery** 8. (1) A person shall not knowingly or without lawful excuse or justification, interfere with data or an electronic system so that he, she, or another person uses

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	the data or the electronic system to induce a person to accept it as genuine and by reason of so accepting it to do or not to do any act to his or her own or any other person's prejudice or injury. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding three years or to both. **Spoof of spam** 17.—(1) A person shall not knowingly or without lawful excuse or justification establish a website or send an electronic message with a counterfeit source– (a) so that the recipient or visitor of an electronic system will believe it to be an authentic source; or (b) to attract or solicit a person or electronic system; for the purpose of gaining unauthorized access to commit a further offence or obtain information which can be used for unlawful purposes. (2) A person shall not knowingly or without lawful excuse or justification– (a) initiate the transmission of multiple electronic mail messages from or through an electronic system; (b) use a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages; or (c) materially falsify header information in multiple electronic mail messages and initiate the transmission of such messages. (3) A person who contravenes subsection (1) or (2) commits an offence and is liable on summary conviction to a fi ne not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years or to both.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system,	**Electronic Crimes Act 2013** **Electronic fraud** 9. (1) A person shall not knowingly or without lawful excuse or justification gain, interfere with data or an electronic system – (a) to induce another person to enter into a relationship; (b) with intent to deceive another person; or (c) with intent to defraud a person,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	where such an act is likely to cause damage or harm to that person or any other person. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding three years or to both.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**Electronic Crimes Act 2013** **2.** In this Act– "child pornography" means pornographic material that depicts, presents or represents– (a) a child engaged in sexually explicit conduct; or (b) an image however so created representing a child engaged in sexually explicit conduct; **Child pornography** 12. (1) For the purposes of this section a "child" means a person who is under the age of eighteen years. (2) A person shall not knowingly and without lawful justification or excuse– (a) publish or transmit or cause to be published or transmitted material in an electronic form which depicts a child engaged in sexually explicit act or conduct; (b) create text or digital images, collect, seek, browse, download, advertise, promote, exchange or distribute material in an electronic form depicting a child in obscene or indecent or sexually explicit manner; (c) cultivate, entice or induce children to an online relationship with another child or an adult for a sexually explicit act or in a manner that may offend a reasonable adult on the electronic system; (d) facilitate the abuse of a child online; (e) record or own in an electronic form material which depicts the abuse of a child engaged in a sexually explicit act; (f) procure and/ or obtain child pornography through a computer system; or (g) obtain access through information and communication technologies, to child pornography. (3) It is a defence to a charge of an offence under subsection (2) paragraphs (f) and (g) if the person can establish that the child pornography was for a bona fide law enforcement purpose. (4) A person who contravenes subsection (2) commits an offence and is liable on conviction on indictment to a fine not exceeding two hundred thousand dollars or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	to a term of imprisonment not exceeding five years or to both and in the event of second or subsequent conviction to a fine not exceeding three hundred thousand dollars or to a term of imprisonment not exceeding twenty years or to both. (5) Subsection (2) does not apply to a book, pamphlet, paper, drawing, painting, representation or figure or writing in an electronic form– (a) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or (b) which is kept or used for bona fide heritage or religious purposes.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	Copyright Act no 21 of 2011

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	General provisions of the Criminal Code (Titles IV and V)
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	General provisions of the Criminal Code
Article 13 – Sanctions and measures	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	**Electronic Crimes Act 2013** **Limited use of data and information** 27. A person shall not without lawful excuse or justification use or disclose data obtained pursuant to this Part for any purpose other than that for which the data was originally sought except– (a) in accordance with any other enactment; (b) in compliance with an order of the Judge in Chambers; (c) where the data is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, assessing or collecting tax, duty or other monies owed or payable to the Government; (d) for the prevention of injury or other damage to the health of a person or serious loss or damage to property; or (e) in the public interest.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of	**Electronic Crimes Act 2013** **Preservation order** 19. (1) Upon evidence sworn to by a police officer of the rank of Inspector, or above an application may be made to a Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of an electronic system, where there are reasonable grounds to believe that the data is vulnerable to loss or modification and where such data is required for the purposes of a criminal investigation or the prosecution of an offence. (2) For the purposes of subsection (1), data includes traffic data and subscriber information.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(3) An order made under subsection (1) remains in force– (a) for a period of thirty days; (b) where prosecution is instituted, until the final determination of the case; or (c) until such time as the Judge in Chambers determines necessary. (4) The period specified for an order granted pursuant to sub-section (1) may be extended, upon an application by the applicant for a further of thirty days or period as may be specified in the order.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Electronic Crimes Act 2013** **Disclosure of preserved data order** 20. For the purposes of a criminal investigation or the prosecution of an offence, upon evidence sworn to by a police officer of the rank of Inspector, or above an application may be made to a Judge in Chambers for an order for the disclosure of– (a) any preserved data, irrespective of whether one or more service providers were involved in the transmission of the data; (b) sufficient data to identify the service providers and the path through which the data was transmitted; or (c) the electronic key enabling access to or the interpretation of data.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.	**Electronic Crimes Act 2013** **Production order** 21. (1) If the disclosure of data is required for the purpose of a criminal investigation or the prosecution of an offence, a police officer not below the rank of Inspector shall make a request of– (a) a person to submit specified data in that person's possession or control, which is stored in an electronic system; (b) a service provider offering its services to submit subscriber information in relation to the services in that service provider's possession and control.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	(2) Where any material to which an investigation relates consists of data stored in an electronic system, disc, cassette, or on microfilm or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible, audible or legible. (3) A person or service provider who refuses to produce the information under subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding one hundred thousand dollars. **Electronic Crimes Act, 2013** "subscriber" means a person listed as using the services of a service provider; "subscriber information" means any information contained in any form that is held by a service provider, relating to subscribers of its services other than traffi c data and by which can be established– (a) the type of communication service used, the technical provisions taken thereto and the period of service; (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or (c) any other information on the site of the installation of communication equipment, 274 Act 23 Electronic Crimes 2013 available on the basis of the service agreement or arrangement; **Electronic Evidence Act, 2013** "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, and by which can be established– (a) the type of communication service used, the technical provisions taken thereto, and the period of service; (b) the subscriber's identity, postal or geographic address, telephone and other information that is capable of identifying the subscriber billing and payment information, as it is available on the basis of the service agreement or arrangement; and (c) any information regarding the location of installed communications equipment as disclosed in the service agreement or arrangement;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Electronic Crimes Act 2013** **Powers of access, search and seizure for the purpose of investigation** 22. (1) Upon evidence sown by a police officer not below the rank of Inspector, that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, the police officer may apply to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize that data. (2) In the execution of a warrant under subsection (1), the powers of the police officer shall include the power to– (a) access, inspect and check the operation of an electronic system; (b) use or cause to be used an electronic system to search any data contained in or available to the electronic system; (c) access any information, code or technology which has the capability of transforming or unscrambling encrypted data contained or available to an electronic system into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which is disclosed in the course of the lawful exercise of the powers under this section; (d) require a person in possession of the decryption information to grant the police officer access to such decryption information necessary to decrypt data required for required for the purpose of investigating the offence; (e) seize or secure an electronic system. (3) A person shall not knowingly or without lawful excuse or justification – (a) obstruct a police officer in the exercise of the police officer's powers under this section; or (b) fail to comply with a request made by a police officer under this section. (4) A person who contravenes subsection (1) commits a summary offence and is liable on summary conviction to a fine not exceeding ten thousand dollars or to a term of imprisonment not exceeding one year or to both. (5) For the purposes of this section– "decryption information" means information or technology that enables a person to readily re-transform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version; "encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable and incomprehensible format, regardless of the technique utilized for transformation or scrambling, and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data; and "plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:	**Electronic Crimes Act 2013** **Real time collection of traffic data**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	23. Where a police officer not below the rank of inspector has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, the police officer may apply to a Judge in Chambers for an order– (a) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of an electronic system; or (b) compelling a service provider, within its technical capabilities to effect such collection and recording referred to in paragraph (a) or assist the police officer to effect such collection and recording. **Mobile phone tracking in emergencies.** 24. (1) A mobile phone service provider shall provide mobile phone tracking to the law enforcement agencies upon request in cases of emergencies with respect to the mobile phone of a person involved in such emergency. (2) Pursuant to subsection (1), cases of emergency include cases of accidents, missing persons and the pursuit of suspects involved in murder, rape, kidnapping or any indictable offence punishable by at least five years imprisonment or more. (3) A mobile phone provider who contravenes subsection (1) commits an offence and is liable on summary conviction to a fi ne of twenty fi ve thousand dollars.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Electronic Crimes Act 2013** **Application** 3. This Act applies where– (a) an offence under this Act was committed in Grenada; (b) any act of preparation towards an offence under this Act or any part of the offence was committed in Grenada or where any result of the offence has had an effect in Grenada; (c) an offence under this Act was committed by a Grenadian national or a person resident or carrying out business in Grenada or visiting Grenada or staying in transit in Grenada; (d) an offence under this Act was committed in relation to or connected with an electronic system or data in Grenada or capable of being connected, sent to, used by or with an electronic system in Grenada; or (e) an offence under this Act was committed by any person, of any nationality or citizenship or in any place outside or inside Grenada, having an effect on the security of Grenada or its nationals, or having universal application under international law, custom and usage

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and	**Electronic Crimes Act 2013** Extraditable offences. 30. An offence pursuant to Part II shall be considered to be extraditable crimes for which extradition may be granted or obtained under the **Extradition Act** Cap. 98.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.	**Mutual Legal Assistance in Criminal Matters Act, no.14 od 2001** https://laws.gov.gd/index.php?option=com_edocman&task=document.download&id=1391&Itemid=193 An Act to make provision for mutual legal assistance in criminal matters between Grenada and designated countries. **2. interpretation** "designated country" means— (a) any Commonwealth country; and (b) any non-Commonwealth country designated by the Minister by order under section 4, and includes any dependent territory of such a country; **4. Designation of countries** (1) Every Commonwealth country is deemed to be designated for the purposes of this Act by virtue of the Harare Scheme Relating to Mutual Assistance in Criminal Matters in the Commonwealth. (2) The Minister may, by order published in the Gazette, designate any non-Commonwealth country for the purposes of this Act, being a country with which Grenada has entered into a bilateral agreement for mutual legal assistance in criminal matters or which is a party to a multilateral scheme or agreement which provides for such assistance and to which Grenada is also a party. (3) The Minister may in an order designating a non-Commonwealth country direct

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	that the application of this Act in relation to the country is subject to the conditions, exceptions or qualifications specified the order, and in that event this Act applies accordingly. (4) The Minister may by order direct that the application of this Act in relation to a particular Commonwealth country is subject to the conditions, exceptions or qualifications specified in the order and in that event this Act applies accordingly. **5. Act not to affect existing forms of co-operation** (1) Nothing in this Act derogates from existing forms of co-operation (whether formal or informal) or prevents the development of other forms of co-operation in respect of criminal matters, between Grenada and any designated country or any other countrywith which Grenada has similar reciprocal arrangements for mutual assistance in criminal matters, or between Grenada or any law enforcement agency or prosecution authority in Grenada and the International Criminal Police Organisation (INTERPOL) or any such agency or authority outside Grenada. (2) Nothing in this Act is to be construed as authorising the extradition, or the arrest and detention with the view to extradition, of any person. **PART III** **Requests by Designated Countries to Grenada for Assistance** **16. Contents of a request** (1) Subject to subsection (2), the provisions of the Schedule apply in relation to a request to Grenada for assistance under this Act by a designated country. (2) Subsection (1) does not apply in relation to an informal request for assistance under this Act which is transmitted orally, but if such a request is accepted— (*a*) it may be implemented only to the extent that the Central Authority of Grenada considers reasonable; and (*b*) it is deemed to have been withdrawn if a request in accordance with subsection (1) for the assistance is not transmitted within a period the Central Authority considers reasonable and notifies to the requesting country. **17. Co-operation in relation to requests for assistance** (1) Subject to this Act, a request for assistance under this Act by a designated country must be granted and executed as expeditiously as possible. (2) The Central Authority of Grenada must inform the designated country making the request of any reason— (a) for not granting or executing the request expeditiously; or (b) for delaying the granting or execution of the request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	18. Refusal of assistance (1) The Central Authority of Grenada may refuse to grant or to execute in whole or in part a request for assistance under this Act if the criminal matter appears to the Central Authority of Grenada to concern— (a) conduct which would not constitute an offence under the laws of Grenada; (b) an offence or proceedings of a political character; (c) conduct which in the country making the request is an offence only under military laws or a law relating to military obligations; (d) conduct which, if it had occurred in Grenada, would have constituted an offence under the military laws of Grenada but which is not also an offence under the ordinary criminal laws of Grenada; or (e) conduct in relation to which the person accused or suspected of having committed the offence has been acquitted or convicted by a court in Grenada. (2) For the purposes of this subsection, an offence is not of a political character if it is an offence within the scope of an international convention to which both Grenada and the country making the request are parties, and which imposes on the parties to it an obligation either to extradite or prosecute a person accused of the commission of the offence, or otherwise afford to one another mutual assistance in criminal matters. (3) The Central Authority of Grenada may refuse to grant or execute a request for assistance under this Act— (a) to the extent that it appears to the Central Authority of Grenada that granting or executing the request would be contrary to the Constitution, or would prejudice the security, international relations or other essential public interests of Grenada; or (b) if there are substantial grounds for the Central Authority of Grenada to believe that granting or executing the request would facilitate the prosecution or punishment of any person on account of his or her race, religion, nationality or political opinions or would cause prejudice for any of those reasons to any person affected by the request. (4) The Central Authority of Grenada may refuse to grant or execute in whole or in part a request for assistance to the extent that the steps required to be taken in order to comply with the request cannot, under the laws of Grenada, be taken in respect of criminal matters in Grenada. (5) If a request for assistance under this Act made by a designated country, other than an informal request, is refused, the fact of, and the grounds for, refusal must be communicated by the Central Authority of Grenada to the Central Authority of that designated country.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Schedule **MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS ACT** ***Requests*** **[Section 16(1).]** **1.** A request to Grenada for assistance under this Act by a designated country must— (*a*) be made by the Central Authority of the requesting country; (*b*) be directed to the Central Authority of Grenada; (*c*) identify the person, agency or authority presenting the request; (*d*) identify the authority conducting the investigation, prosecution or proceedings in the requesting country; (*e*) describe the basis upon which the request is made (i.e. treaty, scheme or agreement); (*f*) describe the nature of the criminal matter, and whether or not criminal proceedings have been instituted; (*g*) describe the relevant facts of the case including, to the extent possible, the alleged offender(s) and the evidence or information so far obtained; (*h*) give a legal description of the offence and the applicable penalty, with copies of the relevant law of the requesting country; (*i*) specify the nature of the assistance required, with precise details of the evidence sought; (*j*) state the connection between the investigation, prosecution or proceedings and the assistance sought, i.e. a description of how the information or evidence sought is relevant to the case; (*k*) describe the procedures to be followed by Grenada's authorities when gathering or transmitting the evidence or assistance requested so that it will serve the purpose for which it was requested. For example, for the taking of testimony, describe the manner in which the testimony should be taken and recorded (for example, summary, verbatim, videotaped, under oath) and whether the requesting country's authorities wish to participate and why. For documentary evidence, any special certification or authentication procedures to be followed should be specified; (*l*) in the case of a request for search and seizure, or for the production of documents, state the basis to believe that the information sought will be found and will afford evidence with respect to the case and describe the documents or items to be searched for and seized or produced. The location or custodian of the records or other evidence should be specified where possible. The description of the documentation sought should include the types of records, as well as the relevant time periods for the records;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(*m*) in the case of a request for a statement or testimony, state the identification and location of the person from whom the evidence is to be obtained, list the topics to be covered and specify the questions to be asked; (*n*) indicate any time-limit within which compliance with the request is desired, giving reasons; (*o*) set out any other information available to the Central Authority of the requesting country to facilitate execution of the request; (*p*) otherwise comply with any relevant bilateral agreement or multilateral agreement or scheme relating to mutual legal assistance. **2.** (1) If the assistance requested is for the purposes of an investigation, the request must— (*a*) be accompanied by the certificate referred to in paragraph (*a*) of the definition of "criminal matter" in section 2(1); and (*b*) include an indication as to when the investigation commenced and the nature of the investigation. (*b*) If the assistance requested is for the purposes of criminal proceedings already instituted, the request must— (*a*) be accompanied by the certificate referred to in paragraph (*b*) of the definition of "criminal matter" in section 2(1); (*b*) give details of the proceedings and the offence concerned, including a summary of the known facts; (*c*) give the identity, if known, of the accused person or the person to whom the proceedings relate; (*d*) state when the proceedings were instituted, the stage reached in the proceedings and any date fixed for further stages in proceedings; and (*e*) state the court exercising jurisdiction in the proceedings. (*c*) If the assistance requested is in connection with or for the purpose of section 28, the request must, as appropriate, be accompanied by a copy of the relevant order and must contain, so far as reasonably practicable, all information available to the Central Authority making the request in connection with the procedure to be followed in Grenada. (*d*) If the assistance requested is for criminal proceedings which have not yet been instituted, the request must state the offence which the Central Authority of the requesting country has reasonable cause to believe to have been committed, with a summary of known facts. **3.** A request must normally be in writing and, if made orally due to urgency, must be confirmed in writing forthwith.
Article 26 – Spontaneous information	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.	**Mutual Legal Assistance in Criminal Matters Act, no.14 od 2001** **3. Central Authority of Grenada** (1) Subject to subsection (2), the Attorney-General is the Central Authority of Grenada. (2) The Attorney-General may in writing authorise another public officer to act as the Central Authority of Grenada generally or in respect of any particular request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	**Mutual Legal Assistance in Criminal Matters Act, no.14 od 2001** **PART II** **Requests by Grenada to Designated Countries for Assistance** **12. Restriction on use of evidence** Any— (*a*) evidence or information obtained or as the case may be given or provided by any person pursuant to a request under section 6 or 9; or (*b*) article, record or thing obtained pursuant to a request under section 6 or 8, must be used by or on behalf of Grenada only for the purposes of the criminal proceedings to which the request relates or, as the case may be, any criminal proceedings resulting from the investigation to which the request relates, unless the designated country to which the request is made consents to the evidence or information being used for the purposes of any other criminal proceedings. **PART III** **Requests by Designated Countries to Grenada for Assistance** **20. Confidentiality** The Central Authority and other competent authorities of a designated country making a request for assistance under this Act must use their best efforts to keep confidential a request and its contents and the information and materials supplied in compliance with a request, except for disclosure in criminal proceedings and as otherwise authorised by the laws of Grenada.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system,	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Mutual Legal Assistance in Criminal Matters Act, no.14 od 2001** PART II Requests by Grenada to Designated Countries for Assistance 6. Assistance in obtaining evidence (1) If there are reasonable grounds to believe that evidence or information relevant to any criminal matter in Grenada may be obtained if, in a designated country action as described in subsection (2) is taken, the Central Authority of Grenada may transmit to the designated country a request for assistance in taking that action. (2) The action referred to in subsection (1) is any or all of the following— (a) taking evidence from a person; (b) providing information; (c) subjecting to examination or test any—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(i) person, (ii) sample, specimen or other item from, or provided by a person, (iii) remains which are, or which may be, human; (d) producing, copying or examining any judicial or official records; (e) producing, copying or examining any record or article; (f) taking, examining or testing samples of any matter or thing; (g) viewing or photographing any building, place or thing. **8. Assistance in obtaining, searching for or seizing articles or things** (1) If there are reasonable grounds to believe that an article or thing is in any designated country which would, if produced, be relevant to any criminal matter in Grenada, the Central Authority of Grenada may transmit to the designated country a request for assistance in obtaining, by search and seizure if necessary, the article or thing. (2) A request under subsection (1) must specify the article or thing to be searched for and seized and must contain, so far as reasonably practicable, all information available to the Central Authority of Grenada which may need to be adduced in an application under the law of that designated country for any necessary warrant or authorisation to affect the search and seizure. **PART III** ***Requests by Designated Countries to Grenada for Assistance*** **21. Assistance to country in obtaining evidence** (1) This section applies where a request is transmitted seeking assistance from Grenada in obtaining, by any of the means specified in section 6, evidence or information relevant to any criminal matter in a designated country, and the request is not refused. (2) Subject to this section, the regulations may prescribe practices and procedures for obtaining evidence or information pursuant to a request for assistance under this section by a designated country. (3) Without limiting section 19(1) a person from whom evidence is taken in Grenada pursuant to a request by a designated country for assistance under this section— (*a*) may refuse to answer any question if— (i) the refusal is based on the laws of Grenada, (ii) to answer the question would constitute a breach of a privilege recognised by the laws of the designated country,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iii) to answer the question would constitute the commission by a person of an offence against the laws of the designated country; and (*b*) must not be compelled to give or provide evidence or information for the purposes of, or in connection with, any criminal matter other than that to which the request relates. (4) In granting or executing a request for assistance under this section, records not publicly available may be produced, copied or examined only to the extent that they could be produced to, or examined by, law enforcement agencies or prosecuting or judicial authorities in Grenada. **23. Assistance to country in obtaining article or thing** (1) This section applies where a request is transmitted seeking assistance from Grenada in obtaining, by search and seizure if necessary, an article or thing in Grenada for the purposes of, or in connection with, any criminal matter in a designated country, and the request is not refused. (2) If this section applies, the Central Authority of Grenada must, unless the article or thing concerned is otherwise lawfully obtainable, apply, or authorise any police officer in writing to apply, to a magistrate having jurisdiction in the area where the article or thing is believed to be located for a search warrant in respect of the article or thing. (3) The laws of Grenada relating to the procedure for— (*a*) the making and disposal of an application for a search warrant; and (*b*) the execution of a search warrant, apply, so far as they are capable of applying, to an application under subsection (2) and to the execution of any warrant issued pursuant to any such application. (4) The Central Authority of Grenada must provide any certification required by the Central Authority of a designated country making a request to which this section applies concerning the result of any search, the place and circumstances of any seizure, and the subsequent custody of any property seized. (5) If this section applies, the Minister may, in writing, authorise any article or thing obtained pursuant to a request to be removed or sent to the designated country that made the request.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents